IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware Corporation, Defendants and Counterclaim-Plaintiffs.	)	C.A. No. 04-1199-SLR

DEFENDANT ISS'S BRIEF IN SUPPORT OF ITS MOTION FOR JUDGMENT AS A MATTER OF LAW AND A NEW TRIAL REGARDING NON-INFRINGEMENT AND INVALIDITY

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
Charles A. Pannell, III
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600

Scott T. Weingaertner
Allison H. Altersohn
KING & SPALDING LLP
1185 Avenue of the Americas
New York, NY 10036
Tel: (212) 556-2100

Adam M. Conrad
KING & SPALDING LLP
One Morrocroft Centre
6805 Morrison Blvd, Suite 200
Charlotte, NC 28211
Tel: (704) 503-2600

Richard L. Horwitz (#2246)
David E. Moore (#3983)
POTTER ANDERSON & CORROON LLP
Hercules Plaza 6th Floor
1313 N. Market Street
Wilmington, DE 19801
Tel: (302) 984-6000
rhorwitz@potteranderson.com
dmoore@potteranderson.com

Attorneys for Defendants
INTERNET SECURITY SYSTEMS, INC., a Delaware corporation; and
INTERNET SECURITY SYSTEMS, INC., a Georgia corporation

Dated: November 17, 2008

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statues and Rules

STATEMENT OF THE CASE

On August 26, 2004, Plaintiff SRI International, Inc. ("SRI") filed this patent infringement suit against Defendants Internet Security Systems, Inc. ("ISS") and Symantec Corporation ("Symantec"). SRI alleged that the Defendants infringed United States Patent Nos. 6,708,212 ("the '212 patent"); 6,484,203 ("the '203 patent"); 6,711,615 ("the '615 patent"); and 6,321,338 ("the '338 patent").

In October 2006, this Court held on summary judgment that Symantec did not infringe the '338 patent and that all four asserted patents were invalid pursuant to 35 U.S.C. § 102. On appeal, the Federal Circuit remanded the case after holding that there was a genuine issue of material fact whether the prior art reference used to invalidate the '203, '615, and '338 patents was a printed publication under Section 102.[1]

From September 2, 2008 until September 17, 2008, the parties tried their infringement and invalidity cases to a jury. During trial, SRI accused ISS of infringing claims 1, 13, 14, and 16 of the '615 patent; claims 1 and 12 of the '203 patent; and claims 1, 11, 12, 13, and 24 of the '338 patent. ISS argued that it did not infringe and that the asserted claims were invalid. On September 17, 2008, the jury returned a verdict that ISS directly infringed and induced the infringement of the asserted claims of the '203 and '615 patents; that ISS did not directly infringe or induce the infringement of the '338 patent; and that all asserted claims of the three patents were valid. D.I. 558.

On October 14, 2008, ISS renewed its motion for judgment as a matter of law and for a new trial on the issues of infringement of the '203 and '615 patents and invalidity of all three patents. D.I. 565. ISS now submits this brief in support of that motion and asks the Court to

---

[1] The Federal Circuit affirmed this Court's ruling that the '212 patent was invalid in view of a second prior art reference.

hold that ISS does not infringe any asserted claim of the '203 and '615 patents and that the '338 patent is invalid as a matter of law. Alternatively, ISS asks this Court to grant ISS's motion for new trial on these issues. ISS and Symantec's joint brief in support of their motions for post trial relief regarding the invalidity of the '203 and '615 patents is filed concurrently herewith.

SUMMARY OF THE ARGUMENT

A) NON-INFRINGEMENT OF THE '615 AND '203 PATENTS

There is no real dispute of fact regarding the evidence of alleged infringement here; the primary dispute lies in SRI's misinterpretation of what it takes to prove infringement and its failure to provide any evidence of intent. SRI has accused the specific combination and use of certain separate ISS software and/or hardware products of infringing and inducing the infringement of the '615 and '203 patents. Specifically, SRI alleges that ISS directly infringes by selling a combination of ISS sensors, its SiteProtector software, and an optional feature of an add-on software package known as Fusion 2.0's Attack Pattern Component ("APC"). SRI also specifically accuses ISS of inducing infringement when customers install and use that combination of products and features on enterprise computer networks. SRI's entire evidentiary theory, however, relies on a legal argument that it only needs to prove ISS's products are "capable of" infringement, not that they have actually infringed, and that evidence of intent to induce acts, not intent to induce infringements, is sufficient to establish the intent prong of their inducement claims. Both theories have been rejected by the Federal Circuit, and SRI's evidence fails to support an infringement finding as a matter of law.

First, to prove direct infringement under 35 U.S.C. § 271(a) a patentee must present evidence that the accused product itself practices every limitation of the asserted claim exactly. In these two patents, the claims are virtually identical and in relevant part require that the

monitors actually be "deployed within an enterprise network," "generat[e] reports of suspicious activity," and "adapted to automatically receive and integrate the reports." In other words, to actually practice the claim, the components must actually be installed and functioning in an enterprise network in the manner claimed, not simply "capable of" being installed and functioning that way if configured in a certain manner. SRI's expert admitted at trial that there is no evidence ISS actually did this deployment and configuration in an enterprise network and instead relied on a mistaken presumption that infringement could be proven if the devices were "capable of" deployment or were "likely" deployed in the claimed manner. With neither circumstantial nor direct evidence of actual deployment by ISS, ISS cannot directly infringe as a matter of law.

Second, with regard to inducement, SRI must provide substantial evidence of both (1) direct infringement by an ISS customer, and (2) that ISS knowingly induced infringement and possessed specific intent to encourage another's infringement. Where an accused product has alternative non-infringing uses, the patentee must prove a specific instance of use in the infringing manner. Despite investigating numerous ISS customers during discovery, the only evidence of customer use presented at trial was the deposition of Mr. Ferrill from HealthSouth. However, while Mr. Ferrill testified that HealthSouth had installed ISS sensors, its SiteProtector software, and an unspecified version of the Fusion add-on module, SRI did not present any evidence--through Mr. Ferrill or otherwise--that HealthSouth ever installed or used the accused 2.0 version of Fusion and, more specifically, the accused Fusion 2.0 Attack Pattern Component. In fact, the only evidence at trial relating to actual use of Fusion by HealthSouth was in relation to the Impact Analysis Component ("IAC"), which is a separately installed component available in the earlier 1.x versions of Fusion and is not accused of infringement. SRI's expert admits that

there was no evidence HealthSouth had installed or used the accused APC component. Again, SRI attempts to rely on the same "capable of" arguments and pure speculation that a customer could potentially install the APC of Fusion and use it in the manner claimed. Not only is speculation generally insufficient to prove infringement, SRI's speculation in this case is particularly unfounded because Mr. Ferrill testified that he did not even know what the APC of Fusion was.

As to the intent prong of inducement, SRI failed to demonstrate that ISS had the specific intent to cause its customers to infringe. To demonstrate intent to cause infringement, SRI must prove that ISS knew of the patents and engaged in culpable conduct to encourage this infringement by others. Inducement cannot be found where the only evidence is that ISS intended to cause the *acts* which constitute infringement; it must specifically intend to cause another to infringe. At trial, there was no evidence presented as to whether ISS was aware of the patents before the filing of the litigation. Furthermore, there was no evidence ISS intended to cause its customers to infringe the SRI patents. At most, the evidence suggests that ISS distributed the Fusion software and provided training materials for the optional APC, but that is not sufficient evidence to prove that ISS intended to cause its customers to infringe. At best, this only proves ISS instructed customers how to deploy and use sensors, SiteProtector, and Fusion APC. There is no evidence ISS specifically knew or intended these acts to be infringing.

In addition to Fusion 2.0's APC, SRI also accused ISS's Third Party Module ("TPM") of infringing dependent claim 16 of the '615 patent. For the same reasons mentioned above, there has been no evidence that ISS or its customers actually used the TPM, but even if there was, the TPM does not infringe as a matter of law. The TPM is not located on a "plurality of network

monitors" described in the claims, and it cannot send third-party reports to the Fusion module accused of receiving and integrating suspicious activity reports in the hierarchical monitor.

B) INVALIDITY OF THE '338 PATENT

At trial, ISS argued that the '338 patent is anticipated by the *JiNao Report*, which was written by a team working with the '338 inventors and actually used many of the same statistical detection algorithms used by SRI, which the *JiNao* researchers found on the internet. At trial, the jury held that the '338 patent was valid, a conclusion directly in conflict with the Patent and Trademark Office ("PTO"). In fact, during the trial the PTO issued a final rejection of the '338 patent based on, *inter alia*, the *JiNao Report*. The '338 patent claims a system of receiving network packets and building statistical profiles of short-term and long-term activity that can then be compared to determine whether something suspicious is occurring on a network. During summary judgment, this Court held there was a question whether the *JiNao Report* described a system that created profiles from "at least one measure of the network packets." This fact was thoroughly established at trial and could not be denied by SRI's expert. Instead, SRI argued that *JiNao Report*'s reference to audit logs negated the paper's repeated disclosure and discussion of measuring packet information to create profiles. Expert testimony that is clearly contrary to the explicit text of a reference, however, cannot establish sufficient rebuttal evidence to preclude invalidity.

STATEMENT OF FACTS

This lawsuit involves three separate patents for computer network intrusion technology. The patents generally describe a system that examines a computer network for malicious attacks. All three patents at issue have the same written description. They only differ by what is claimed in each patent.

The parties commonly refer to the '615 and '203 patents as the "hierarchical monitoring" patents because they claim a system composed of "network monitors" that generate reports of suspicious network activity and send those reports to a higher-level "hierarchical monitor." The parties commonly refer to the '338 patent as the "statistical detection" patent because it claims a system that compares short-term and long-term statistical profiles of data to detect suspicious network activity.

A) THE PATENTS-IN-SUIT

1. The '615 and '203 Patents

SRI accused ISS of infringing claims 1, 13, 14, and 16 of the '615 patent and claims 1 and 12 of the '203 patent. The only substantive difference between the claims of the two patents is that the '615 patent claims two additional network traffic data categories. 9/4/08 Tr. 685:21-686:2.[2] In fact, the parties agree that the primary limitations of both the method and system claims are the same. 9/4/08 Tr. 600:11-12.

Independent claim 13 of the '615 patent is representative of the asserted claims:

> 13. An enterprise network monitoring system comprising:
>
> a plurality of network monitors deployed within an enterprise network, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};
>
> said network monitors generating reports of said suspicious activity; and

[2] For simplicity, ISS will refer to the claims and specification of the '615 patent unless otherwise indicated.

one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.

PTX-4 col. 15, l. 56 - col. 16, l. 6 (the underlined categories of network traffic are not claimed in the '203 patent). In addition to independent claim 13, SRI asserted dependent claims 14 and 16:

14. The system of claim 13, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.

16. The system of claim 13, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.

PTX-4 col. 16, l. 7-16.

2. The '338 Patent

During trial, SRI also accused ISS of infringing claims 1, 11, 12, 13, and 24 of the '338 patent. ISS presented evidence at trial that the '338 patent was invalid as anticipated by a technical report authored by Frank Jou, entitled "Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure" ("the *JiNao Report*"). DTX-51. The jury found that ISS did not infringe the '338 patent but that the '338 patent was valid.

The '338 patent essentially claims a system that builds a statistical profile of long-term and short-term network activity, and then compares the profiles to determine if there is suspicious network activity. It is undisputed that the *JiNao Report* is prior art to the '338 patent. JTX-1. The parties' primary dispute turns on whether the *JiNao Report* discloses two elements of independent claims 1 and 24 relating to network packets:

1. A method of network surveillance, comprising:
receiving network packets handled by a network entity;

building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;

comparing at least one long-term and at least one short-term statistical profile; and

determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

PTX-1, '338 Patent, Claim 1 (claim limitations disputed for invalidity purposes are underlined).

B) THE ACCUSED ISS PRODUCTS

Chris Klaus, the founder of ISS, began the company in 1994 in his grandmother's basement. 9/4/08 Tr. 758:11-22. ISS's first product, Internet Security Scanner, was used by companies to detect vulnerabilities in a computer network that made the network susceptible to attack. 9/4/08Tr. 757:24-758:10. As the company grew, ISS also began producing products that helped network administrators detect attacks on computer networks. One of the first such products, RealSecure, was released in 1996 -- almost two years before SRI filed its first intrusion detection patent application. The early RealSecure product consisted of: (1) sensors or engines (i.e., "network monitors"), which monitored network traffic for signs of attacks or suspicious activity and generated reports about such activity; and (2) management software (i.e., the "hierarchical monitor"), which received and integrated reports of suspicious activity from the sensors. 9/4/08 Tr. 763:3-764:4, 769:13-770:2.

Around the turn of the century, ISS developed a new line of sensors and management software. 9/10/08 Tr. 1308:16-19, 1311:3-20. ISS marketed its new sensors under the "Proventia" name, and its new management software under the "SiteProtector" name. 9/4/08 Tr. 638:5-15; 639:6; 644:7-15. In addition to sensors or management software, ISS's customers could also purchase various optional, add-on software modules that provided additional functionality or features to the SiteProtector product. 9/10/08 Tr. 1311:14-20; 9/4/08 Tr. 686:13-18. The SiteProtector SecurityFusion product ("Fusion") is one of the optional, add-on modules that ISS sells. SRI contends that certain Proventia and RealSecure sensors, when used in

combination with the Attack Pattern Component ("APC") of Fusion 2.0, infringe the '203 and '615 patents.[3] 9/4/08 Tr. 709:12-15; 659:25-660:3. Thus, SRI's infringement theory requires the use of three separate ISS products: (1) certain ISS sensors, (2) SiteProtector, and (3) Fusion 2.0's APC.

1. **ISS Sensors**

The accused ISS sensors detect suspicious activity (such as viruses, worms, or hackers) on a computer network.

2. **SiteProtector and the Fusion 2.0 Attack Patten Component**

Fusion 2.0 is an optional add-on module to SiteProtector that can be purchased by ISS's customers. Fusion 2.0 consists of two independently-developed components: (1) the Impact Analysis Component ("IAC"), and (2) the Attack Pattern Component ("APC"). Significantly, a customer must install each of these components separately in order to use them with the SiteProtector product to receive reports from the sensors, 9/4/08 Tr. 702:23-703:9 and customers can use Fusion 2.0 without installing the APC feature, 9/4/08 Tr. 703:1-4.

ISS initially sold the IAC as part of its Fusion 1.0 release in 2001.[4] The IAC compares vulnerability information received from the Internet Security Scanner product to reports about attacks to determine the risk of harm to the network by that type of attack. 9/4/08 Tr. 703:18-25; 705:24-706:2 (noting ISS customer described the IAC); 9/3/08 SEALED p. 15:18-16:14 (ISS customer describing IAC); 9/15/08 Tr. 2009:10-11, 17-18; 9/3/08 Tr. 433:7-11. SRI does not accuse the IAC of infringing the '203 and '615 patents. 9/15/08 Tr. 2009:2-14.

---

[3] SRI also accuses ISS's Third Party Module of infringing dependent claim 16. For simplicity, we have separately addressed the Third Party Module non-infringement in Section (B) 3. of the Argument below.

[4] Fusion 1.0, 1.1, and 1.2 (collectively "Fusion 1.x") did not contain the accused APC component. 9/4/08 Tr. 686: 3-12; 704:14-15.

ISS first released the APC as part of its Fusion 2.0 release in the Spring of 2003. 9/3/08 Tr. 432:23; 9/4/08 703:18-25. The APC module combines different reports from the ISS sensors into certain preprogrammed attack types called "incidents." 9/3/08 Tr. 433-34, 445-46; 429; 9/4/08 Tr. 656-59. A customer must install the APC separately in order to use this functionality as part of the Fusion product. 9/4/08 Tr. 702:23-703:5-9.

For the jury's verdict of infringement to withstand post-trial scrutiny, there must be substantial evidence that either ISS (for direct infringement) or one of its customers (for indirect infringement) (1) deployed a plurality of ISS sensors ("network monitors") within an enterprise network; (2) configured those sensors to generate events ("reports") of suspicious activity; (3) deployed SiteProtector and, specifically, the APC of Fusion 2.0 (the "hierarchical monitor") in the enterprise network; (4) and used the APC to receive and integrate those events ("adapted to receive and integrate"). At trial, SRI did not present any evidence that ISS or any ISS customer ever deployed or used such a system. Moreover, the only evidence of actual use presented at trial was in relation to the use of the non-accused IAC feature of Fusion.

ARGUMENT

A) STANDARD OF REVIEW

Judgment as a matter of law is appropriate if a party has been fully heard on an issue and "there is no legally sufficient evidentiary basis for a reasonable jury to find for that party on that issue." *Bullen v. Chaffinch*, 336 F. Supp. 2d 342, 346 (D. Del. 2004); *see also Novartis Pharms. Corp. v. Abbott Labs.*, 375 F.3d 1328, 1332 (Fed. Cir. 2004) (affirming JMOL of non-infringement). A court should grant judgment as a matter of law "if 'viewing the evidence in the light most favorable to the nonmovant and giving it the advantage of every fair and reasonable inference, there is insufficient evidence from which a jury reasonably could find liability.'"

Buskirk v. Apollo Metals, 307 F.3d 160, 166 (3d Cir. 2002) (quoting *Lightning Lube, Inc. v. Witco Corp.*, 4 F.3d 1153, 1166 (3d Cir. 1993)). At trial, SRI had the burden of proving infringement by a preponderance of the evidence. *Cross Medical Prods., Inc. v. Medtronic Sofamor Danek, Inc.*, 424 F.3d 1293, 1310 (Fed. Cir. 2005). ISS had the burden of proving invalidity by clear and convincing evidence. *Voda v. Cordis Corp.*, 536 F.3d 1311, 1322 (Fed. Cir. 2008).

The decision to grant or deny a new trial is within the sound discretion of the Court, and the Court need not view the evidence in the light most favorable to the verdict winner. *See Allied Chem. Corp. v. Daiflon, Inc.*, 449 U.S. 33, 36 (1980). Federal Rule of Civil Procedure 59(a) provides that the Court may, on motion, grant a new trial "for any reason for which a new trial has heretofore been granted in an action at law in federal court." Fed. R. Civ. P. 59(a).

B) ISS DOES NOT INFRINGE OR INDUCE THE INFRINGEMENT OF THE '615 AND '203 PATENT

SRI has accused ISS of literally[5] infringing the '203 and '615 patents, both directly and indirectly, under 35 U.S.C. §§ 271(a) and 271(b). For the reasons stated below, there was insubstantial evidence presented at trial to establish either theory.

1. SRI's Argument that ISS Directly Infringed the '203 and '615 Patents is Based Upon a Rejected Legal Theory

To establish direct, literal infringement, SRI must present substantial evidence that ISS itself made, used, offered to sell, or sold the patented invention. 35 U.S.C. § 271(a). This means that "every limitation set forth in a claim must be found in [ISS's] accused product, exactly." *Southwall Tech., Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1575 (Fed. Cir. 1995); *see also Cross*

[5] At trial, SRI attempted to argue that ISS's products infringe the asserted claims under the doctrine of equivalents through the bald conclusions of its expert. In the face of Defendants' JMOL motions during trial (D.I. 542 & 543), SRI dropped its doctrine of equivalents claims 9/15/08 Tr. 1959:18-20, and they were not submitted to the jury.

Medical, 424 F.3d at 1310. If ISS itself does not make, use, or sell a product that meets every limitation of the patent, ISS cannot directly infringe. *See id.* at 1311 (holding that because patent claims required apparatus to be joined to bone, only surgeons, not the manufacturer-defendant, could directly infringe); *see also* (Tr. 688:10-16 (noting same legal theory applied by Plaintiff's expert).)

As SRI's expert admitted, there is no evidence that ISS itself actually deployed or used the accused products in a manner that infringed the patent claims. 9/4/08 Tr. 689:16-690:4; *see also* 9/4/08 Tr. 645:5-10 (identifying the only evidence of actual deployment of monitors in an enterprise network was at one of ISS's customers). Instead, SRI argued at trial that ISS's sale of uninstalled ISS sensors, uninstalled SiteProtector software, and uninstalled Fusion 2.0 software meets the limitations of the asserted claims because ISS's products are "capable of" being used in a way that infringes. 9/4/08 Tr. 748:7-23.

The Federal Circuit, however, has rejected SRI's "capable of" infringement theory. *See Cross Medical*, 424 F.3d at 1311; *see also Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1307 (Fed. Cir. 2006) (rejecting capable of argument where system claims required devices to be in a single package).[6] In *Cross Medical*, the patent claim at issue required the interface of an accused medical device to be operatively joined to bone, which meant it must be in contact with bone to practice the claim. 424 F.3d at 1310-11. The defendant, however, only manufactured the device with an interface; it did not perform surgery, so it did not practice the claim limitation requiring contact with bone. Like SRI in this case, the plaintiff in *Cross Medical* argued that the defendant was liable for direct infringement because it manufactured a device that was *capable* of infringement, i.e. capable of being in contact with bone. *Id.* at 1310. The court explicitly

[6] This Court also rejected SRI's "capable of" argument during arguments for its proposed jury instructions at trial. D.I. 544 at 2; 9/12/08 Tr. 1950:11-13.

rejected this argument noting that "[t]o infringe an apparatus claim, the device must meet all of the structural limitations." *Id.* at 1311-12. Thus, because the defendant "[did] not itself make an apparatus with the 'interface' portion in contact with bone, [defendant did] not directly infringe." *Id.* at 1311.[7]

Similarly, the uninstalled products that ISS sells do not themselves practice each asserted claim limitation. This is because the claims require that network monitors (e.g., the ISS sensors) and the adapted hierarchical monitor (e.g., SiteProtector with Fusion 2.0 APC) be "deployed within an enterprise network" and "in the enterprise network," respectively. There is no evidence that ISS sells deployed sensors or hierarchical monitors in an enterprise network because the accused products themselves are not sold deployed within a network. Moreover, the uninstalled ISS sensors do not "detect[] suspicious network activity" or "generat[e] reports," and the uninstalled Fusion APC software does not "receive and integrate the reports." Like the medical device in *Cross Medical* that could not directly infringe until it was implanted in a patient and in contact with bone, the ISS sensors and Fusion APC software cannot infringe until they are actually deployed and operating in an enterprise network. Thus, SRI has failed to present any evidence that ISS directly infringes the patent claims.

2. <u>There Is No Evidence that ISS Induced Infringement of the '203 and '615 Patents</u>

SRI also has failed to present any evidence that ISS has induced the infringement of the '203 and '615 patents. Section 271(b) allows a patentee to hold a party liable for another's direct infringement when that party "actively induces infringement of a patent." To prove infringement by inducement, SRI has the burden of proving "first that there has been direct infringement, and second that the alleged infringer knowingly induced infringement and possessed specific intent

---

[7] SRI agreed at trial that method claims could not be infringed by the same "capable of" argument. D.I. 544 at 2; 9/11/08 Tr. 1636:17-23.

to encourage another's infringement." *ACCO Brands, Inc. v. ABA Locks Manufacturer Co.*, 501 F.3d 1307, 1312 (Fed. Cir. 2007); *accord DSU Med. Corp. v. JMS Co.*, 471 F.3d 1293, 1304 (Fed. Cir. 2006) (en banc). At trial, SRI failed to present sufficient evidence that ISS's customers directly infringe or that ISS knowingly induced infringement with specific intent.

i. SRI Presented No Evidence that Any ISS Customer Directly Infringed the '615 or '203 Patents

"[A]bsent direct infringement of the claims of a patent, there can [not] be . . . inducement of infringement." *Dynacore Holdings Corp. v. U.S. Philips Corp.*, 363 F.3d 1263, 1277 (Fed. Cir. 2004) (citation omitted). To establish direct infringement for inducement purposes, SRI must offer more than "speculation" or "theoretical possibility" that ISS's customers make or use network intrusion detection systems as described in the claims. *Id.* (holding that patentee failed to offer sufficient evidence of any computer network that met all asserted claim limitations); *accord Lucent Techs., Inc. v. Gateway, Inc.*, 543 F.3d 710, 723-24 (Fed. Cir. 2008).

In this case, SRI must prove a specific instance of infringement by an ISS customer. "In order to prove direct infringement, a patentee must either point to specific instances of direct infringement or show that the accused device necessarily infringes the patent in suit." *Lucent Techs., Inc.*, 543 F.3d at 723 (citation omitted); *accord Dynacore*, 363 F.3d at 1275-76. Here, a customer's purchase and use of Fusion does not necessarily infringe the patents. *ACCO*, 501 F.3d at 1313. First, only the 2.0 version of Fusion is accused of infringement; earlier 1.x versions are not accused. Second, the 2.0 version of Fusion contains two separate components, the IAC and the APC, each of which must be separately installed by a customer in order to function. 9/4/08 Tr. 702:23-703:4. SRI's expert conceded that the IAC does not infringe, 9/4/08 Tr. 702:12-14, and that a customer who purchases Fusion 2.0 does not *necessarily* have to install or use the accused APC feature. 9/4/08 Tr. 703:1-17. Thus, SRI was required to present some

specific evidence that a customer actually infringes, i.e., that a customer has installed ISS sensors on an enterprise network and has installed, configured and used the accused Fusion APC feature in the claimed manner.

Despite having obtained discovery from several ISS customers, SRI offered at trial the testimony of only one ISS customer, Mr. Ferrill of HealthSouth, in support of its inducement claim. 9/4/08 Tr. 690:5-691:3. Although Mr. Ferrill testified that he purchased and installed ISS sensors, the SiteProtector software, and an unspecified version of Fusion, 9/3/08 SEALED Tr. 6-8; 9/4/08 Tr. 705:17-19, there was no testimony or other evidence that HealthSouth purchased the accused ***2.0*** version of Fusion, 9/4/08 Tr. 705:17-19, much less installed or used the separate accused Fusion APC feature. 9/4/08 Tr. 706:3-5. In fact, Mr. Ferrill testified that he was not even familiar with the APC feature of Fusion. 9/3/08 SEALED Tr. 14:16; 9/4/08 705:17-706:5. And, when asked how HealthSouth actually used Fusion, Mr. Ferrill only described using the non-infringing IAC component. 9/4/08 Tr. 705:24-706:5; 9/3/08 SEALED Tr. 15:16-16:14. SRI's expert agreed that there was no evidence that HealthSouth actually installed or used the accused Fusion APC feature. 9/4/08 Tr. 705:24-706:5.

Rather than point to a specific instance of infringement as required by law, SRI's expert admitted that his infringement analysis did not rely on evidence of "actual use." 9/4/08 Tr. 748:7-23; *see also* 744:23-745:1 (discussing Symantec infringement).) Instead, Dr. Kesidis admitted that his infringement theory is based on the same rejected "capable of" argument discussed previously in the direct infringement analysis. 9/4/08 Tr. 748:7-23.

Dr. Kesidis' infringement analysis improperly attempts to bootstrap a conclusion based on unsupported assumption and speculation. As he explains, "I'm ***assuming*** that ***if*** the APC was purchased with Fusion, I made an argument that ***it's likely*** that the APC is being used." 9/4/08

Tr. 703, ll.13-15 (emphasis added); *see also* Tr. 749:9-17. This assumption and speculation that an infringing system *may* exist, without pointing to a single network where it *does* exist was explicitly rejected in *Dynacore*. *See Dynacore*, 363 F.3d at 1277 ("Dynacore has not pointed to even a single network that *both* complies with the IEEE 1394 Standard *and* meets the 'equal peers' limitation, nor has Dynacore presented anything other than speculation that such a network might exist." (emphasis in original)); *see also ACCO*, 501 F.3d at 1313-14 ("The mere sale of a product capable of substantial non-infringing uses does not constitute indirect infringement of a patent." (citation and alteration omitted)). If a customer's use of the APC was as "likely" as Dr. Kesidis assumes, it should not have been difficult for SRI to come forward with some evidence that the APC has actually been used in an infringing manner. *See E-Pass Techs., Inc. v. 3COM Corp.*, 473 F.3d 1213, 1222-23 (Fed. Cir. 2007) ("If, as [Plaintiff] argues, it is "unfathomable" that no user in possession of one of the accused devices and its manual has practiced the accused method, E-Pass should have had no difficulty in meeting its burden of proof and in introducing testimony of even one such user." (citation omitted)); *see also Lucent Techs., Inc. v. Gateway, Inc.*, 543 F.3d at 723 (noting the district court's reasoning that if running the accused computer program was "so common and so routine" then the plaintiff could have produced evidence of at least one instance where it had run). SRI's failure to provide either direct or circumstantial evidence of specific infringement by ISS's customers prevents a reasonable jury from finding that ISS induced their infringement under Section 271(b).

ii. SRI Presented No Evidence that ISS Intentionally Induced Infringement

Even if there were substantial evidence of direct infringement by an ISS customer, SRI failed to establish the second prong of an inducement claim -- that ISS intentionally induced that infringement. To prove inducement, SRI "has the burden of showing that the alleged infringer[]

. . . knew or should have known his actions would induce actual infringements." *DSU*, 471 F.3d at 1304. At a minimum, SRI failed to present any evidence at trial that ISS even knew of the patents prior to the suit. Moreover, even if SRI had presented evidence that ISS knew of the patents before the suit, SRI failed to present sufficient evidence that ISS had the specific intent required to induce infringement of those patents.

a. SRI Presented No Evidence that ISS Knew of the Asserted Patents

"The requirement that the alleged infringer knew or should have known his actions would induce actual infringement necessarily includes the requirement that he or she knew of the patent." *Id.* at 1304; *accord Medtronic Vascular, Inc. v. Boston Scientific Corp.*, 348 F. Supp. 2d 316, 323 (D. Del. 2004); *see also Manville Sales Corp. v. Paramount Sys., Inc.*, 917 F.2d 544, 553-54 (Fed. Cir. 1990) (reversing inducement finding when defendants had no knowledge of patent before suit was filed and continued sales with good faith belief that products did not infringe after suit was filed); *cf. Liquid Dynamics Corp. v. Vaughan Co.*, 449 F.3d 1209, 1222-23 (Fed. Cir. 2006) (noting there was no question the infringer knew of patent after first accused sale); *MEMC Electronic Materials, Inc. v. Mitsubishi Materials Silicon Corp.*, 420 F.3d 1369, 1380 (Fed. Cir. 2005) (knowledge of patent established with letter sent to defendant). A review of the trial record reveals no direct or circumstantial evidence that ISS actually knew of the patents prior to the litigation. In the absence of any such evidence, ISS cannot be liable for inducing infringement.

b. SRI Presented No Evidence that ISS Possessed Specific Intent to Induce Infringement

Knowledge of the patents by itself is not enough to prove inducement. *See MEMC*, 420 F.3d at 1380. "[A] patent holder must prove that once the defendants knew of the patent, they 'actively and *knowingly* aid[ed] and abett[ed] another's direct infringement.'" *DSU*, 471 F.3d at

1305 (quoting *Water Techs. Corp. v. Calco, Ltd.*, 850 F.2d 660, 668 (Fed. Cir. 1988)(emphasis and alterations in original)). "However, knowledge of the acts alleged to constitute infringement is not enough." *Id.* at 1305 (citation omitted). There must be some "evidence of culpable conduct, directed to encouraging another's infringement. . . ." *Id.* at 1306.

SRI's reliance on ISS's marketing literature and customer training materials to prove inducement is misguided. The Federal Circuit recently made clear that supplying hardware and software "capable of" infringement and training customers on how to use the components in a way that infringes is not sufficient evidence that the defendant specifically intended infringement. *Kyocera Wireless Corp. v. ITC*, ___ F.3d ___, 2008 WL 4553140, at **10-11 (Fed. Cir. Oct. 14, 2008).

In *Kyocera*, the respondent, Qualcomm, was accused of inducing its customers to infringe a certain power saving computer patent. *Id.* at *1. The patent claimed a computing device that had circuitry that was "adapted to" use two different wireless scan modes to reduce power and conserve battery life. *Id.* The ITC found that Qualcomm's customers directly infringed when they installed system determination software on Qualcomm's chips. *Id.* at *10. However, the Federal Circuit remanded the ITC's findings because the evidence of providing software, literature, and support, among other things "evince[d], at most, a finding that Qualcomm generally intended to cause acts that produced infringement." *Id.* at *11. The record fell short of the required specific intent needed to induce infringement. *Id.*

Like Qualcomm, the fact that ISS sells hardware (e.g., sensors) and software (e.g., Fusion 2.0) that can allegedly cause infringement, and provides instructions and support for using these products in different ways, is insufficient evidence of the specific intent to cause infringement as required by Section 271(b).

3. ISS's Third Party Module Does Not Infringe Claim 16 of the '615 Patent

At trial, SRI further argued that another add-on module, the Third-Party Module ("TPM"), infringes dependent claim 16 of the '615 patent. Since claim 16 depends from claim 13, all limitations of claim 13 must be met as well as the additional limitation of claim 16. Accordingly, ISS reasserts its prior non-infringement arguments for claim 13 here. For several additional reasons, however, SRI has failed to introduce sufficient evidence that ISS infringes claim 16. In particular, SRI has failed to demonstrate that any network monitor, much less the "plurality of network monitors," include an API, or that ISS or any customer purchased or installed the ISS sensors, SiteProtector, Fusion APC, and the TPM.

First, even if the TPM is installed in combination with the ISS sensors, SiteProtector, and Fusion APC, it does not infringe the '615 patent. The TPM is a module that can be added to the SiteProtector software to allow records from several third-party firewall products to be fed into SiteProtector. 9/3/08 Tr. 425:22-427:1; 9/4/08 667:1-4; PTX-204; PTX-205 at SRI 000050. However, TPM is not capable of transmitting reports to the Fusion APC. 9/3/08 Tr. 436:22-437:10; 9/4/08 Tr. 709:9-11. Therefore, the TPM does not integrate third party tools (i.e., the third party reports) or encapsulate monitor functions because those third party reports cannot be analyzed and integrated by the Fusion APC. Moreover, to make this argument, SRI must interpret "plurality of network monitors" to mean only the single unadapted SiteProtector hierarchical monitor. The ISS sensors that supposedly make up the plurality of network monitors for SRI's claim 13 infringement analysis, 9/4/08 Tr. 644:4-15, are not included for the claim 16 infringement analysis. Thus, no reasonable juror could find infringement, even if this Court assumes all of these products were installed in combination.

Second, SRI lacks evidence of direct infringement by ISS or its customers. There is no evidence ISS ever used TPM on an enterprise network with sensors, SiteProtector, and Fusion APC. Furthermore, the only ISS customer presented at trial was Mr. Ferrill of HealthSouth who said he was not familiar with the TPM. 9/4/08 Tr. 476:10-12. This is not sufficient evidence to demonstrate HealthSouth (or any other customer) even purchased TPM, much less installed or used it.

C) '338 PATENT INVALIDITY

ISS further requests that this Court grant judgment as a matter of law that the '338 Patent is anticipated by both the *JiNao Report* and *Analysis of TCP/IP Gateways* ("Live Traffic"). DTX-499 (Porras, P.A. & Valdes, A., *Live Traffic Analysis of TCP/IP Gateways*, Paper submission to the 1998 ISOC Symposium on Network and Distributed System Security, pp. 1-15, Aug. 1997). SRI has conceded that *Live Traffic* anticipates the '338 Patent, JTX-1, ¶17, and the publication of that document has been addressed in Section II. D. 4. of Defendants' Memorandum In Support Of Their Motions For Post Trial Relief Regarding Invalidity Of The '203 And '615 Patents. ISS incorporates the contentions of Defendants' Joint Brief regarding *Live Traffic* herein and discusses invalidity based upon the *JiNao Report* below.

1. The JiNao Report

At trial, Defendants offered the *JiNao Report* as prior art that anticipates the asserted '338 patent claims.[8] The *JiNao Report* describes the architecture of an intrusion detection system that protects against intrusions into network infrastructure, such as routers. *See* DTX-51 at 1. The *JiNao Report* describes a dual analysis engine monitor that is quite similar to the dual

[8] Notably, during trial the Patent and Trademark Office, upon further reexamination of the '338 patent, issued its final rejection of the '338 patent claims by finding them invalid in light of the *JiNao Report*. *See* 11/17/08 Moore Declaration, Exhibit A (PTO Final Rejection 9/5/08).

engine configuration described in the '338 patent. *Compare* DTX-51 Fig. 1 *with* PTX-1 Fig.2. Both monitors receive network traffic and perform statistical analysis upon that traffic looking for intrusions. In addition, both monitors use the same NIDES statistical algorithms for network traffic. *See* PTX-1, Col. 5, ll. 36-52; DTX-51 at 18; 9/11/08 Tr. at 1538:16-1539:19. These similarities are not unexpected; Mr. Jou, the *JiNao Report's* author, was working with SRI and the inventors of the '338 patent over a year before the patents were filed. 9/11/08 Tr. 1503:14-1504:11; 1538:16-1540:4; 1544:9-1546:22.

The *JiNao Report* discloses a system that analyzes network packets. For example, "[a]spects of subject behavior are represented as measures (*e.g., packet and LSA arrival frequencies* in terms of their types or sources)." DTX-51 at 19 (emphasis added); *see also* 9/12/08 Tr. at 1725:21-1726:14 (ISS expert). Indeed, *JiNao* explicitly sets forth statistical formulas for long-term and short-term profiles related to measures of network packets: "The Q statistic compares the short-term distribution *of the types of packets* that have been received with the long-term distribution of the same types." DTX-51 at 21 (emphasis added).

In addition to network packets, the *JiNao Report* also discusses audit records. According to the *JiNao Report*, such audit records are directly derived from network packets. For example, the *JiNao Report* provides a specific example of developing profiles from different types of packets to make up the "audit record distribution measure." DTX-51 at 19; Tr. 1724-27 (ISS expert describing this passage). According to the *JiNao Report*, "[t]he audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State

Update packets, and 20 of Acknowledgment packets." DTX-51 at 19. Thus, even when discussing audit records, the *JiNao Report* discloses that its measures are taken from the underlying network packets.

2. The Jury's Verdict on the Validity of the '338 Patent Is Not Supported by Substantial Evidence

SRI attempted to rebut Defendants' evidence of invalidity with the testimony of its expert, Dr. Kesidis, who testified that the *JiNao Report* does not anticipate the '338 patent. As recognized by this Court on summary judgment, the parties' primary dispute is whether the *JiNao Report* builds statistical profiles from "at least one measure of the network packets." D.I. 525 at 8.[9]

Dr. Kesidis testified that the *JiNao Report* only "relies on audit records rather than raw packet traffic to perform intrusion detection." 9/12/08 Tr. 1829:25 - 1830:1. However, Dr. Kesidis's argument is contradicted by the explicit teaching of the *JiNao Report* itself. *See Motorola, Inc. v. Interdigital Tech. Corp.*, 121 F.3d 1461, 1473 (Fed. Cir. 1997) (stating that an expert's "presumed knowledge does not grant a license to read into the prior art reference teachings that are not there"); *see also Brooke Group Ltd. v. Brown & Williamson Tobacco Corp.*, 509 U.S. 209, 242 (1993) ("When an expert opinion is not supported by sufficient facts to validate it in the eyes of the law, or when indisputable record facts contradict or otherwise render the opinion unreasonable, it cannot support a jury's verdict."). Moreover, even if accepted as true, Dr. Kesidis's admissions confirm a finding of invalidity.

[9] Dr. Kesidis admitted that the *JiNao Report* created long- and short-term profiles. 9/15/08 Tr. 2001:20-21; *see also* D.I. 525 at 8 (Court Order on Summary Judgment).

i. Dr. Kesidis's Testimony That the JiNao Report Does Not Disclose Measures of Network Packets Is Factually Inaccurate

As an initial matter, it must be noted that Dr. Kesidis admitted that the JiNao system received network packets. 9/12/08 Tr. 1886:18. In his own words, the JiNao system is a "host-based *system of packets you receive* and transmit . . . ." 9/12/08 Tr. 1890:16-17. Later, Dr. Kesidis confirmed JiNao was receiving packets. 9/12/08 Tr. 1898:17-18 ("the packets, the information that JiNao is receiving . . . ").

Nevertheless, Dr. Kesidis concluded that the JiNao system did not take measures of the received packets. Ignoring the *JiNao Report's* repeated references to packets and measures of such packets *see, e.g.*, DTX-51 at 19, 21-22, Dr. Kesidis focused narrowly on the term "audit log." He testified that *JiNao* converted the received network packets into protocol data units ("PDU"), which he called a type of audit log format. 9/12/08 Tr. 1888:21-1889:20. According to Dr. Kesidis, the local detection module of the JiNao system "performs protocol and statistical analysis on the auto [sic] logs that are a result of the routing message being processed." 9/12/08 Tr. 1887:1-3; *see also* Tr. at 1889:23-24. Again, although acknowledging that the JiNao system received network packets, Dr. Kesidis asserted that the system performed analysis only on audit logs, stating "any host-based system of packets you receive and transmit are going to have some impact on your audit log and JiNao is no different here. So they're audit transcripts inside the router that are being analyzed . . . ." 9/12/08 Tr. 1890:16-21.

As shown above, however, the *JiNao Report* refutes this testimony in clear and unambiguous terms. Furthermore, the *JiNao Report* explicitly describes the statistical formulas for its long-term and short-term profiles, which related to a "*distribution of the types of packets* that have been received" -- that is, measures of the received network packets. DTX-51 at 21 (describing the Q statistic) (emphasis added). In light of these unambiguous statements from the

reference itself, no reasonable jury could credit Dr. Kesidis's factually inaccurate and contradictory conclusions. *See Upjohn Co. v. MOVA Pharmaceutical Corp.*, 225 F.3d 1306, 1311 (Fed. Cir. 2000) ("[T]here must be factual support for an expert's conclusory opinion.").

ii. Even if Dr. Kesidis's Testimony Is True, the JiNao System's Audit Logs Are Measures of Network Packets

In addition to being contrary to the *JiNao Report*, Dr. Kesidis's focus on "audit log" language, as opposed to "packet" language, is beside the point for at least two reasons. First, a reference's mention of or even preference for alternative modes of operation does not preclude anticipation of a patent claim, so long as it discloses the claimed mode of operation. *Glaxo Group Ltd. v. Apotex, Inc.*, 376 F.3d 1339, 1348 (Fed. Cir. 2004) ("[A]nticipation requires that all limitations of the claimed invention are described in a single reference, rather than a single example in the reference." (citation omitted)). Thus, the *JiNao Report's* references to measures of network packets alone suffice to invalidate the '338 patent, irrespective of other passages in the report that refer to audit records.

Second, even if the *JiNao Report* could be interpreted to disclose only measures taken from audit records, such audit records are directly derived from network packets -- a fact acknowledged by Dr. Kesidis. 9/12/08 Tr. 1889:13-14 ("So you're taking the raw packets and you're transforming them into the PDU format . . . .").) Indeed, although the *JiNao Report* labels one of its measures as an "audit record distribution measure," the term refers to a measure of network packets. DTX-51 at 19 ("For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment packets."); 9/12/08 Tr. 1724-27 (ISS expert). As shown above, the Q statistic for the "audit record distribution measure" compares "the short-term distribution *of the types of packets* that have

been received with the long-term distribution of the same types." DTX-51 at 21 (emphasis added). Even accepting Dr. Kesidis's testimony, the resulting measures are not measures of the audit logs; they are measures of the underlying network packets even if the packet data resides in a router-log format.[10]

Furthermore, Dr. Kesidis's testimony is at war with his conclusion. According to Dr. Kesidis, network packets are sent through the "extraction layer" of the prevention module of the JiNao system: "Again, *the raw information here is the raw packets*. So you're taking the raw packets and you're transforming them into the PDU format, and accepted by the detection module through a generic interface." 9/12/08 Tr. 1889:12-15 (emphasis added). When asked about JiNao's statistical measures, Dr. Kesidis stated that "what's clearly happening here is that *the inference of a packet type is made* by examination of an audit record, not by looking at the packet whizzing by and the raw on the wire." 9/12/08 Tr. 1893:7-10 (emphasis added). In this testimony, Dr. Kesidis inappropriately draws an unwritten limitation into the claim language. The claim requires only that the profile be built with "measure[s] of the network packets"; it does not claim *raw* network packets. Moreover, through each of these statements, it is apparent -- even from Dr. Kesidis's view -- that the JiNao system not only received network packets but also then made "inference[s]" (that is, analyses) about those packets. In Dr. Kesidis's own words, the information being measured in the JiNao system *comes from packets*.

---

[10] There is ample reason to suggest that the *JiNao Report* used the terms "packets" and "audit records" interchangeably. As Mr. Smaha explained, in the *JiNao Report,* "some of these equations have variables in them, which are described sometimes as audit records and sometimes as packets, and he uses the same variable names with either term to refer to them. So from that, I will conclude that since he's using the two different terms to refer to the same stuff, that he means the same thing by them." 9/12/08 Tr. 1727:20 - 1728:1. Although Dr. Kesidis challenged Mr. Smaha's testimony, he did so only in conclusory testimony and asserted no basis for that opinion. 9/12/08 Tr. 1894:17 - 1895:3. No reasonable jury could conclude that network packets and measures of network packets were not being described here.

iii. The JiNao System Discloses the Dependent Hierarchical Limitations

Finally, in regards to the separate dependent claims asserted, ISS's expert Mr. Smaha testified that the *JiNao Report* discloses the hierarchical limitations of the asserted dependent claims. 9/12/08 Tr. 1732:17 - 1733:20. In conclusory testimony, however, Dr. Kesidis asserted that the *JiNao Report* does not disclose the dependent limitations:

> "Q. Do you agree that the Ji Nao report discloses a monitor that can send reports to hierarchically higher monitor, as that is recited and claimed in the '338, Claim 13?
> A. No.
> Q. Why not?
> A. Well, it doesn't, (A). . . ."

9/12/08 Tr. 1897:23 - 1898:4. At no point did Dr. Kesidis ever support his conclusion with the *JiNao Report*. Rather, he supports his opinion with characterizations of deposition testimony by Frank Jou. 9/12/08 Tr. 1898:4-9. Without factual support, Dr. Kesidis's testimony cannot support the jury's verdict. *See Upjohn*, 225 F.3d at 1311.

In sum, the *JiNao Report* plainly contradicts Dr. Kesidis's conclusory testimony and discloses that statistical profiles are built from measures of network packets. Even if a reasonable jury could ignore the clear statements from the *JiNao Report* itself, Dr. Kesidis's own testimony establishes the '338 patent's invalidity.

D) MOTION FOR NEW TRIAL

In the alternative to judgment as a matter of law, ISS requests a new trial on the issues of infringement of the '203 and '615 patents and the validity of the '338 patent. The Court has considerable discretion to grant a new trial and need not view the evidence in the light most favorable to the verdict winner. *See Lucent Techs., Inc. v. Newbridge Networks Corp.*, 168 F. Supp. 2d 181, 251 (D. Del. 2001); *see also* Fed. R. Civ. P. 59(a)(1)(A). In this case, a new trial is warranted because the jury's verdict is against the clear weight of the evidence, as shown

above, and a new trial must be granted to prevent a miscarriage of justice. *See Lucent Techs.*, 168 F. Supp. 2d at 251 (citing *Zarrow-Smith v. N.J. Transit Rail Operations*, 953 F. Supp. 581, 584 (D. N.J. 1997)). In addition, ISS incorporates by reference the additional grounds raised in Section III. C. of Defendants' Opening Brief in Support of Their Motions for Post Trial Relief Regarding Invalidity of the '203 and '615 Patents, filed the same day as the instant brief. For these reasons, if the Court chooses not to grant judgment as a matter of law, ISS respectfully requests a new trial on the verdicts against it.

CONCLUSION

For the abovementioned reasons, SRI has failed to submit sufficient evidence to meet its burden of proof that ISS has infringed or induced the infringement of the '615 and '203 patents, and failed to submit any substantial evidence to rebut ISS's overwhelming evidence that the *JiNao Report* and *Live Traffic* anticipate the '338 patent. Accordingly, ISS asks this Court to grant its motion for judgment as a matter of law, or alternative motion for new trial, that ISS does not infringe the '615 and '203 patents and that the '338 patent is invalid. In the alternative, ISS asks this Court to grant it a new trial on the verdicts against it.

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
Charles A. Pannell, III
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600

Scott T. Weingaertner
Allison H. Altersohn
KING & SPALDING LLP
1185 Avenue of the Americas
New York, NY 10036
Tel: (212) 556-2100

Adam M. Conrad
KING & SPALDING LLP
One Morrocroft Centre
6805 Morrison Blvd, Suite 200
Charlotte, NC 28211
Tel: (704) 503-2600

Dated: November 17, 2008
891748 / 28434

POTTER ANDERSON & CORROON LLP

By: */s/ David E. Moore*
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza 6th Floor
1313 N. Market Street
Wilmington, DE 19801
Tel: (302) 984-6000
rhorwitz@potteranderson.com
dmoore@potteranderson.com

Attorneys for Defendants
INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation; and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia corporation

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, David E. Moore, hereby certify that on November 17, 2008, the attached document was electronically filed with the Clerk of the Court using CM/ECF which will send notification to the registered attorney(s) of record that the document has been filed and is available for viewing and downloading.

I further certify that on November 17, 2008, the attached document was Electronically Mailed to the following person(s):

Thomas L. Halkowski
Kyle Wagner Compton
Fish & Richardson P.C.
222 Delaware Avenue, 17th Floor
P.O. Box 1114
Wilmington, DE 19899-1114
halkowski@fr.com
kcompton@fr.com

Richard K. Herrmann
Mary B. Matterer
Morris James LLP
500 Delaware Avenue, Suite 1500
Wilmington, DE 19899
rherrmann@morrisjames.com
mmatterer@morrisjames.com

Howard G. Pollack
Steven C. Carlson
John N. Farrell
Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, CA 94063
pollack@fr.com
steven.carlson@fr.com
jfarrell@fr.com

Paul S. Grewal
Renee DuBord Brown
Katie J.L. Scott
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd, Suite 400
Cupertino, CA 95014
pgrewal@daycasebeer.com
rbrown@daycasebeer.com
kscott@daycasebeer.com

/s/ David E. Moore
Richard L. Horwitz
David E. Moore
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 North Market Street
Wilmington, DE 19899-0951
(302) 984-6000
rhorwitz@potteranderson.com
dmoore@potteranderson.com

683314 / 28434